

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-290389

(43)Date of publication of application : 04.10.2002

---

(51)Int.Cl. H04L 9/08  
G06F 17/60

---

(21)Application number : 2001-084298 (71)Applicant : HITACHI LTD

(22)Date of filing : 23.03.2001 (72)Inventor : SHIRAISHI MASAHI  
IWASAKI KAZUMASA  
KOBAYASHI RIE  
KOIKE HIROSHI  
HATOOKA JUNICHI

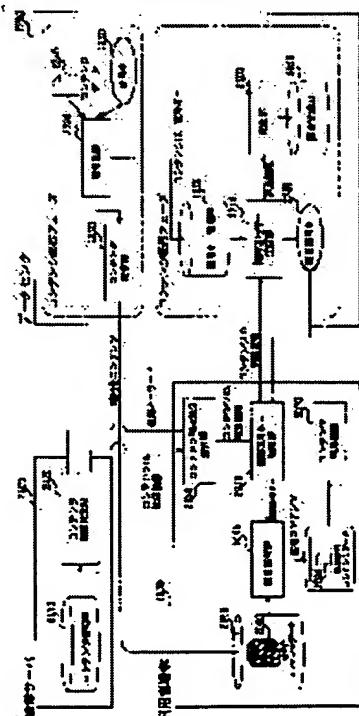
---

## (54) DATA DECODING METHOD, DATA DECODER, AND DATA SALES SYSTEM

## (57)Abstract:

PROBLEM TO BE SOLVED: To provide a data decoding method and device that decodes encrypted data only for a partial range of the data when the encrypted data are decoded and to provide a data sales system that decodes encrypted data having been given to a user in advance only for part of the data desirably used by the user and can impose the utility charge of the limited data part only onto the user.

SOLUTION: A decoding key used to decode data whose partial range is selected and utilized such as video, music or electronic book data includes a key to decode the entire data and partial range information for decoding. In the case of decoding the data, only the partial range data included in the decoding key are decoded and outputted. Furthermore, in a contents data sales system, only a specific range as above is decoded, a decoding key to decode only a required part of encrypted data by a user and distributed in advance to the user is produced, only the required part of the encrypted data is decoded by using the decoding key and the decoded data are provided to the user, and the decoding key is sold to impose the utility charge of the required part only



onto the user.

---

#### LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2002-290389  
(P2002-290389A)

(43)公開日 平成14年10月4日 (2002.10.4)

(51)Int.Cl. <sup>7</sup> H 04 L 9/08 G 06 F 17/60	識別記号 5 1 2	F I G 06 F 17/60 H 04 L 9/00	テ-マコ-ト(参考) 5 1 2 5 J 1 0 4 6 0 1 B
---	---------------	------------------------------------	--

審査請求 未請求 請求項の数11 O.L (全21頁)

(21)出願番号 特願2001-84298(P2001-84298)

(22)出願日 平成13年3月23日 (2001.3.23)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 白石 匡央

神奈川県川崎市幸区鹿島田890番地 株式  
会社日立製作所ビジネスソリューション事  
業部内

(74)代理人 100096954

弁理士 矢島 保夫

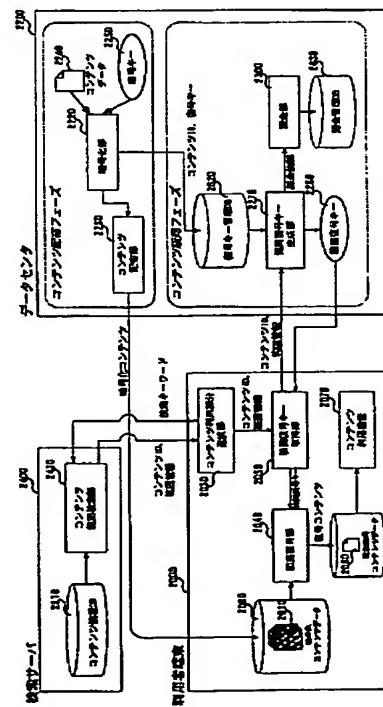
最終頁に続く

(54)【発明の名称】 データ復号化方法、データ復号化装置、およびデータ販売システム

## (57)【要約】

【課題】暗号化データの復号化においてデータの部分範囲に限って復号化を行うデータ復号方法及び装置を提供するとともに、あらかじめ利用者に渡された暗号化データに対し、そのデータの利用したい部分のみを復号化して利用させ、同時にその部分のみの利用料を課金することができるデータ販売システムを提供することを目的とする。

【解決手段】映像や音楽、または電子書籍のデータのように、その部分範囲を選択して利用できるデータに対し、これを復号する復号キーの中にデータ全体を復号するキーと復号する部分範囲情報を含ませる。データ復号時には復号キーに含まれる部分範囲のみを復号化し出力する。また、コンテンツデータ販売システムにおいて、このような特定の範囲のみを復号化するようにし、利用者にあらかじめ配布された暗号化データに対して、利用者が必要とする部分のみを復号する復号キーを作成し、その復号キーにより暗号化データの中の利用部分のみを復号化して利用者に提供して、その復号キーを販売することにより利用部分のみの利用料を課金する。



## 【特許請求の範囲】

【請求項 1】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、暗号化されたデータはその暗号化の前または後のいずれかの状態において部分範囲を選択可能なデータであり、選択された部分範囲の復号化データを取得するために与えられる範囲復号キーは、前記暗号化されたデータの全体または一部分を復号するための復号キーと復号範囲情報とを含み、前記暗号化されたデータに対して前記復号キーを用いて範囲復号処理を施すことにより、前記復号範囲情報で指定された部分範囲のみの復号化データを出力することを特徴とするデータ復号化方法。

【請求項 2】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、前記暗号化されたデータは、それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号化されたデータの部分範囲を選択可能なものであり、前記暗号化されたデータ中の選択された部分範囲の復号化の処理は、前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中の復号すべき部分として選択された部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、前記暗号化されたデータ中の前記復号範囲情報で指定される部分範囲のみを、前記復号キーを用いて、復号化するステップと、復号化した前記部分範囲のデータを出力するステップとを備えていることを特徴とするデータ復号化方法。

【請求項 3】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、前記暗号化されたデータは、その全体が 1 つの復号キーで復号化できる 1 つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであり、前記暗号化されたデータの選択された部分範囲の復号化の処理は、前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、前記暗号化されたデータ全体を、前記復号キーを用いて、復号化するステップと、復号化したデータ中の前記復号範囲情報で指定された部分範囲のみを復号化データとして出力するステップとを備えていることを特徴とするデータ復号化方法。

【請求項 4】請求項 1 から 3 の何れか 1 つに記載のデータ復号化方法において、前記復号キーには、復号キー発行元の電子署名を付加し、データの復号化時に該電子署名を検定することを特

徴とするデータ復号化方法。

【請求項 5】請求項 1 から 4 の何れか 1 つに記載のデータ復号化方法において、前記復号キーは、復号キー発行元と復号化装置とが共有する秘密キーで暗号化してあることを特徴とするデータ復号化方法。

【請求項 6】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化装置であって、復号化の対象である前記暗号化されたデータは、それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号化されたデータの部分範囲を選択可能なものであり、前記暗号化されたデータ中の選択された部分範囲の復号化を行うため、前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中の復号すべき部分として選択された部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力する手段と、前記暗号化されたデータ中の前記復号範囲情報で指定される部分範囲のみを、前記復号キーを用いて、復号化する手段と、復号化した前記部分範囲のデータを出力する手段とを備えたことを特徴とするデータ復号化装置。

【請求項 7】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化装置であって、復号化の対象である前記暗号化されたデータは、その全体が 1 つの復号キーで復号化できる 1 つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであり、前記暗号化されたデータの選択された部分範囲の復号化を行うため、前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力する手段と、

前記暗号化されたデータ全体を、前記復号キーを用いて、復号化する手段と、復号化したデータ中の前記復号範囲情報で指定された部分範囲のみを復号化データとして出力する手段とを備えたことを特徴とするデータ復号化装置。

【請求項 8】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化プログラムであって、それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号化されたデータの部分範囲を選択可能なものであるような暗号化されたデータを復号化の対象とし、前記暗号化されたデータ中の選択された部分範囲の復号化の処理として、前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中

の復号すべき部分として選択された部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、

前記暗号化されたデータ中の前記復号範囲情報で指定される部分範囲のみを、前記復号キーを用いて、復号化するステップと、

復号化した前記部分範囲のデータを出力するステップとを備えていることを特徴とするデータ復号化プログラム。

【請求項9】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化プログラムであって、

その全体が1つの復号キーで復号化できる1つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであるような暗号化されたデータを復号化の対象とし、

前記暗号化されたデータの選択された部分範囲の復号化の処理として、

前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、

前記暗号化されたデータ全体を、前記復号キーを用いて、復号化するステップと、

復号化したデータ中の前記復号範囲情報で指定された部分範囲のみを復号化データとして出力するステップとを備えていることを特徴とするデータ復号化プログラム。

【請求項10】コンテンツデータを管理するデータセンタと、ネットワーク経由で該データセンタに接続し前記コンテンツデータを購入する利用者端末とを備えたデータ販売システムであって、

前記利用者端末は、

利用者があらかじめ取得している暗号化データに対して、該データ中の利用部分の範囲を選択する手段と、選択された利用部分の範囲を復号化するための範囲復号キーを前記データセンタに要求する手段と、

前記要求に応じて前記データセンタから送信される範囲復号キーを取得する手段と、

取得した範囲復号キーを用いて前記暗号化データの利用部分の範囲を復号化し、該利用部分の範囲の復号化データのみを出力する手段とを備え、

前記データセンタは、

前記利用者端末からの要求に応じて、前記利用部分の範囲を復号化するための範囲復号キーを生成して、前記利用者端末に送信する手段を備えたことを特徴とするデータ販売システム。

【請求項11】請求項10に記載のデータ販売システムにおいて、

前記データセンタは、前記範囲復号キーの生成に連携して、該利用部分の範囲に応じた課金を行う手段を、さらに備えたことを特徴とするデータ販売システム。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、暗号化データを復号化する技術に関し、特に、部分範囲を選択可能なデータを扱うデータ復号化方法および装置、並びに暗号化データを復号する復号キーを販売するデータ販売システムに関する。

##### 【0002】

【従来の技術】ネットワーク、特にインターネットを用いたオンライン販売システムにおいて、アプリケーションソフトウェアや、または書籍や映像、音楽などのデータをデジタル化したデータなどのいわゆるデジタルコンテンツの販売が行われている。これらの販売システムでは、ネットワークにより販売データの配達を行う「データのダウンロード販売」が行われている。

【0003】デジタルコンテンツデータは簡単にコピーできてしまうため、コンテンツ販売システムにおいては、コンテンツの不正使用防止を目的としてコンテンツデータに対し暗号化処理を施すことが行われている。ここで、暗号化とはデータの使用にあたって復号手続きを必要とするようにデータの状態を変えることを示している。一般的な暗号化方法のDES (Data Encryption Standard) やRSAなどだけでなく、例えばデジタル映像データに対し可視透かしを入れたり、デジタル音楽データに対しある種のノイズを挿入するなど、データの品質を下げる加工を施し、そしてその状態を解除し品質の高いデータに復元することができるデータ変換処理もここでは暗号化方法とみなす。

【0004】デジタルコンテンツのダウンロード販売において、映像や音楽などのデータサイズが大きいデジタルコンテンツを扱う場合にはそのダウンロード待ち時間が問題になる。この待ち時間を縮小するため、利用者に対しデジタルコンテンツデータをあらかじめ配布しておく方法がある。あらかじめ配布されるコンテンツデータは暗号化されており、利用者はデータの利用時に暗号を解除する復号キーを購入し、復号キーを用いて暗号を解除してコンテンツデータを利用する。例えば、シェアウェアのソフトウェアは機能制限版をCD-ROMなどで配布し、利用者はソフトウェアの制限を解除するキーを購入し、機能制限を解除して使用することができる。

【0005】あらかじめ配布した暗号化データに対し復号キーを販売するシステムでは、復号キーの漏洩や複製、または捏造などにより不正にデータを復号化し利用されてしまうことによって、データ利用料を正しく課金することができなくなる問題がある。このため、データに対する暗号化処理・復号化処理の方法には特に配慮がなされている。例えば、特開平11-39262号公報に示されるように、あらかじめ配布された暗号化データを復号化する際、利用者の端末側の端末情報を暗号化してデータを管理するデータセンタへ送付し、データセン

タでは暗号化された端末情報を復号化し、それを利用者端末で復号化できる形式で暗号化して利用者端末へ送り返す。利用者端末では送り返された暗号化情報を復号化し、それと最初に送った端末情報を比較し、一致している場合のみあらかじめ配布されたデータの復号化を行う。この技術では、あらかじめ配布された暗号化データを復号化する際に、前に利用者端末とデータセンタの間で相互の認証を厳密に行うことができる。

#### 【0006】

【発明が解決しようとする課題】あらかじめ暗号化データを配布する前記従来の方法においては、次のような問題がある。

【0007】デジタルコンテンツのデータとして映像や、音楽、書籍などのデータは、そのデータの任意の部分範囲を選択して利用したいことがある。例えば、映像・音楽データの場合、データの始めから30秒間分だけのデータを利用することや、また書籍データの場合、本の中のある章だけ利用することなどである。暗号化コンテンツデータを配布し、それを復号化して利用させる前記のデータ販売方法において、販売対象のコンテンツとして上述の任意の部分範囲を選択できるコンテンツデータを扱うためには、暗号化データから任意の部分範囲のみを復号化する手段が必要となる。しかし、従来の暗号データの復号化方法では暗号化データを任意の部分範囲のみを復号化することはできず、データの全範囲を復号化してしまう問題がある。

【0008】この復号化の問題により、前記のデータ販売方法において利用者が部分範囲を使用したいと申請した場合に、利用させたくない部分を含む全範囲のデータを復号化し利用可能とさせてしまう問題がある。この際の課金において、部分範囲の利用料のみを課金した場合には、販売者と利用者の間で申請範囲以外の部分の不正利用を行わないように信用取引的な面が生じてしまい、また全範囲分の利用料を課金する場合は、使用しない部分の料金を払わなければならなくなり、単価の高いデータなどでは利用者にとって負担が大きくなる問題がある。

【0009】本発明は、上述の従来技術における問題点に鑑み、暗号化データの復号化においてデータの部分範囲に限って復号化を行うデータ復号方法及び装置を提供するとともに、あらかじめ利用者に渡された暗号化データに対し、そのデータの利用したい部分のみを復号化して利用させ、同時にその部分のみの利用料を課金することができるデータ販売システムを提供することを目的とする。

#### 【0010】

【課題を解決するための手段】上記目的を達成するため、本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、暗号化されたデータはその暗号化の前または後のいずれか

の状態において部分範囲を選択可能なデータであり、選択された部分範囲の復号化データを取得するために与えられる範囲復号キーは、前記暗号化されたデータの全体または一部分を復号するための復号キーと復号範囲情報とを含み、前記暗号化されたデータに対して前記復号キーを用いて範囲復号処理を施すことにより、前記復号範囲情報で指定された部分範囲のみの復号化データを出力することを特徴とする。

【0011】また本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、前記暗号化されたデータは、それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号化されたデータの部分範囲を選択可能なものであり、前記暗号化されたデータ中の選択された部分範囲の復号化の処理は、前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中の復号すべき部分として選択された部分範囲を指定する復号範囲情報を含む範囲復号キーを入力するステップと、前記暗号化されたデータ中の前記復号範囲情報を指定される部分範囲のみを、前記復号キーを用いて、復号化するステップと、復号化した前記部分範囲のデータを出力するステップとを備えていることを特徴とする。

【0012】また本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、前記暗号化されたデータは、その全体が1つの復号キーで復号化できる1つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであり、前記暗号化されたデータの選択された部分範囲の復号化の処理は、前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報を含む範囲復号キーを入力するステップと、前記暗号化されたデータ全体を、前記復号キーを用いて、復号化するステップと、復号化したデータ中の前記復号範囲情報を指定された部分範囲のみを復号化データとして出力するステップとを備えていることを特徴とする。

【0013】また本発明は、上述のデータ復号化方法において、前記復号キーには、復号キー発行元の電子署名を付加し、データの復号化時に該電子署名を検定することを特徴とする。

【0014】また本発明は、上述のデータ復号化方法において、前記復号キーは、復号キー発行元と復号化装置とが共有する秘密キーで暗号化してあることを特徴とする。

【0015】さらに本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化装置であって、復号化の対象である前記暗号化されたデータは、それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号

化されたデータの部分範囲を選択可能なものであり、前記暗号化されたデータ中の選択された部分範囲の復号化を行うため、前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中の復号すべき部分として選択された部分範囲を指定する復号範囲情報を含む範囲復号キーを入力する手段と、前記暗号化されたデータ中の前記復号範囲情報を指定される部分範囲のみを、前記復号キーを用いて、復号化する手段と、復号化した前記部分範囲のデータを出力する手段とを備えたことを特徴とする。

【0016】また本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化装置であって、復号化の対象である前記暗号化されたデータは、その全体が1つの復号キーで復号化できる1つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであり、前記暗号化されたデータの選択された部分範囲の復号化を行うため、前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報を含む範囲復号キーを入力する手段と、前記暗号化されたデータ全体を、前記復号キーを用いて、復号化する手段と、復号化したデータ中の前記復号範囲情報を指定された部分範囲のみを復号化データとして出力する手段とを備えたことを特徴とする。

【0017】さらに本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化プログラムであって、それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号化されたデータの部分範囲を選択可能なものであるような暗号化されたデータを復号化の対象とし、前記暗号化されたデータ中の選択された部分範囲の復号化の処理として、前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中の復号すべき部分として選択された部分範囲を指定する復号範囲情報を含む範囲復号キーを入力する手段と、前記暗号化されたデータ中の前記復号範囲情報を指定される部分範囲のみを、前記復号キーを用いて、復号化する手段と、復号化した前記部分範囲のデータを出力する手段とを備えていることを特徴とする。

【0018】また本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化プログラムであって、その全体が1つの復号キーで復号化できる1つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであるような暗号化されたデータを復号化の対象とし、前記暗号化されたデータの選択された部分範囲の復号化の処理として、前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報を含む範囲復号キーを入力する手段と、

前記暗号化されたデータ全体を、前記復号キーを用いて、復号化するステップと、復号化したデータ中の前記復号範囲情報を指定された部分範囲のみを復号化データとして出力するステップとを備えていることを特徴とする。

【0019】さらに本発明は、コンテンツデータを管理するデータセンタと、ネットワーク経由で該データセンタに接続し前記コンテンツデータを購入する利用者端末とを備えたデータ販売システムであって、前記利用者端末は、利用者があらかじめ取得している暗号化データに対して、該データ中の利用部分の範囲を選択する手段と、選択された利用部分の範囲を復号化するための範囲復号キーを前記データセンタに要求する手段と、前記要求に応じて前記データセンタから送信される範囲復号キーを取得する手段と、取得した範囲復号キーを用いて前記暗号化データの利用部分の範囲を復号化し、該利用部分の範囲の復号化データのみを出力する手段とを備え、前記データセンタは、前記利用者端末からの要求に応じて、前記利用部分の範囲を復号化するための範囲復号キーを生成して、前記利用者端末に送信する手段を備えたことを特徴とする。

【0020】また本発明は、上述のデータ販売システムにおいて、前記データセンタは、前記範囲復号キーの生成に連携して、該利用部分の範囲に応じた課金を行う手段を、さらに備えたことを特徴とする。

【0021】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

【0022】図1は、本発明の第1の実施形態のデータ復号化方法とそれに用いる暗号化データと復号キーの概念を示す。範囲復号装置1220は、暗号化データ1200と範囲復号キー1260を入力とし、範囲復号キー1260の中の復号範囲1030で示される暗号化データ1200の部分範囲のみを復号化して、復号化範囲データ1250を出力する。

【0023】暗号化データ1200は、その暗号化データ自身またはその暗号化前の元データが、論理的にまたは物理的にその部分範囲を選択できるデータである。例えば、データとして電子書籍データを考えた場合には、ページ番号を用いて電子書籍データの部分範囲を選択することができる。また、映像データを考えた場合には、映像の開始時間と終了時間を指定することで、映像データの部分範囲を選択することができる。さらに、前記のような時間やページ番号で順序付けられた連続データの部分範囲を選択することだけでなく、例えば同一内容を示す英語、日本語、ドイツ語、および中国語の文書を総めて管理する複合文書データの中から日本語の文書だけを選択することもデータの部分範囲の選択である。また、写真集のデータのように、複数の写真データの集合データの中からキーワード「夕日」に合う写真データを

選択するようなことも、データの部分範囲の選択である。

【0024】暗号化データ1200は、ある部分単位の暗号化データ1280の集合として表されており、それぞれの部分単位の暗号化データ1280は全て同一キーで復号化できるように暗号化されている。例えば、暗号化データ1200として、電子書籍のデータを考える場合、ページごとに同一キーで暗号化したページデータの集合として表すことができる。また、映像データを考える場合、個々のフレーム画像を同一キーで暗号化したフレーム画像データの集合として表すことができる。また、前記写真集の暗号化データも、個々の写真を同一キーで暗号化したデータの集合として表されている。つまり、ここでいう部分単位とは、電子書籍データの場合は各ページのデータに相当し、映像データの場合は各フレーム画像のデータに相当するものである。暗号化データ1200は、写真集データのように部分単位暗号化データ1280の個々のファイルの集合と表されることもあれば、映像データのように1つの映像データファイル、例えばMPEGファイルのような形のこともある。映像ファイルの場合は、1つのファイルの中に複数のフレーム画像のデータを含んでおり、フレーム画像集合を纏めたファイルとみなすことができる。

【0025】本実施形態のデータ復号化方法は、上述したような、あるデータの中からその部分データを選択できるようなデータを対象とするものである。

【0026】図1において、範囲復号キー1260は、何れの部分単位の暗号化データをも復号できる全体復号キー1270と、データの中からその部分範囲を選択する復号範囲情報1030とを含んでいる。復号範囲情報1030は、例えば、暗号化データ1200が電子書籍データの場合なら開始ページ番号と終了ページ番号であり、暗号化データ1200が映像データなら開始時間と終了時間である。全体復号キー1270は、個々の暗号化部分データ1280を復号する共通の復号キーである。復号化範囲データ1250は、暗号化データ1200の中の復号範囲情報1030で選択された部分範囲1210を復号化したデータである。

【0027】範囲復号装置1220は、範囲選択部1230と復号化部1240を備える。範囲選択部1230は、部分単位暗号データ1280の集合である暗号化データ1200の中から、範囲復号キー1260の中の復号範囲情報1030に従い、選択範囲データ1210を抜き出す。例えば、暗号化したページデータの集合として表される電子書籍のデータの場合には、開始ページ番号と終了ページ番号で構成される復号範囲情報1030で指定されたページのみを選択し出力する。また、個々のフレーム画像が暗号化された映像データの場合は、開始時間と終了時間で構成される復号範囲情報1030で指定された時間区間に含まれるフレーム画像を抜き出し

出力する。復号化部1240は、選択範囲データ1210の個々のデータ1290に対し、範囲復号キー1260に含まれる全体復号キー1270を用いてデータの復号化を行い、復号化範囲データ1250を出力する。

【0028】図1では、復号化範囲データ1250として復号化した部分単位データのみを出力しているが、これは暗号化データ1200全体の中で復号範囲1210のみを復号化したデータ集合として出力しても良い。例えば、30分の暗号化映像データに対し、復号範囲1030で示される区間が先頭から10分を示していた場合、先頭から10分のみの映像データを出力する形態もあれば、先頭から10分のみが視聴できる状態になっている30分の映像データとして出力する形態もある。

【0029】暗号化データ1200の中の部分集合1210のみを復号化する方法として、部分単位データをそれぞれ別々のキーで暗号化し、復号化時に復号範囲に対応する部分単位データの復号キーを全て渡すようするような方法が考えられる。しかし、この方法では、範囲復号キー1260に全ての復号キーを含めなければならない、復号範囲の大きさに比例して長くなってしまう。また、全ての部分単位データに対する復号キーを管理しなければならない問題がある。例えば、映像のフレーム画像に対し前記方法を探るならば、映像1秒当たり30枚のフレーム画像があるため、1時間の映像の場合では10万個のキーを管理しなければならない。本実施形態によれば、1つの映像、すなわちフレーム画像の集合データに対し1つのキーを管理するだけでよく、範囲復号キーには1つの全体復号キーを含ませるだけで部分範囲の復号化を行うことができる。

【0030】図2は、本実施形態のデータ復号化方法を用いたコンテンツデータ販売システムの構成を示す図である。以降では、このシステムにおけるデータ販売の処理手順を用いて本実施形態のデータ復号化方法を説明する。本実施形態のコンテンツ販売システムは、ネットワーク2500に接続された、利用者端末2000、データセンタ2200、及び検索サーバ2400を備える。利用者端末2000はネットワーク2500を介してコンテンツを購入し、利用するための装置である。データセンタ2200は、コンテンツを利用する利用者に対しコンテンツデータの配布とコンテンツデータの利用による課金を行う。検索サーバ2400は、利用者がコンテンツデータ購入のために欲しいコンテンツを検索したいとき、利用者に検索機能を提供する装置である。

【0031】利用者端末2000は、コンテンツデータの復号処理や利用などのためのプログラムを格納する二次記憶装置2010、暗号化コンテンツデータを格納する二次記憶装置2080、メモリ2100、CPU2110、及びネットワークインターフェース2120を備えており、これら各部はバス2130で接続されている。

【0032】二次記憶装置2080に格納される暗号化

コンテンツデータ2090は、あらかじめ利用者に配布されたデータである。一般的なデータダウンロード販売の方式として、利用者のデータ利用時に、オーデマンドにデータセンタからコンテンツデータをダウンロードする方式がある。これに対し、本実施形態の方式では、事前に利用者に対しコンテンツデータを配布している。これにより、利用者のデータ利用時のデータダウンロード待ち時間を減らすことができる。

【0033】コンテンツデータの事前配布方法は、例えばCD-ROM、あるいはDVD-ROMなどの大容量メディアにコンテンツデータを格納し、それらを陸送などで配布すればよい。ある程度の量のコンテンツデータを纏めて配布することにより、ネットワーク転送よりも陸送の方がデータ転送のコストを安く抑えることができる。また別のデータ配布方法として、利用者がネットワークを使用していない時間等に、利用者の利用要求とは非同期にデータの転送を行う方法もある。

【0034】どのコンテンツデータを配布するかに対しては、データセンタが管理する全てのコンテンツデータを配布する方法が考えられる。このようにすれば、コンテンツデータのダウンロード時間は0にできる。しかし、実際には全てのデータを送付することはデータ量から考えると難しく、事前配布するデータは配布可能な量だけを選択して配布することになる。この場合、事前配布されたデータはキャッシュ的に使われるようになる。すなわち、利用者の希望するデータが、既に配布されている場合はそれを用い、配布されていない場合はデータセンタ2200からダウンロードする。利用者に対し事前に配布するコンテンツデータの決め方は、過去のデータ利用統計により人気の高いデータを送付したり、利用者に対し事前にアンケートをとり、その結果から興味がありそうなデータを送付するなどの方法がある。

【0035】データ配布方法の別の形態として、広帯域ネットワークでデータセンタと接続されたコンテンツデータの販売端末から、ある程度纏めた量のデータを一括でダウンロードしておく方法などもある。この場合に、例えば電子書籍のデータに対して、ある本の一部だけを使用したいという利用者の要求に対し、販売端末からは本全体のデータをダウンロードさせて、その中の利用したい部分だけを使用させることができる。利用者がその本の別の部分を利用したいときには、その本の当該範囲を復号化する復号キーを購入することにより利用できる。これにより、データのダウンロード時間が必要ななくなる。

【0036】これら事前に配布するコンテンツデータは、利用者による料金の支払いより前にデータが渡される。そのため、利用者に料金を払っていないコンテンツデータを利用させないように、データに暗号化を施しておく必要がある。

【0037】二次記憶装置2010には、オペレーティ

ングシステム（以下、OSと記述する）2020、利用者が暗号化コンテンツデータ2090の利用する部分を選択するためのコンテンツ利用部分選択部2030、データセンタ2200にコンテンツ利用部分を復号するためのキーを要求する範囲復号キー取得部2050、範囲復号キーを用いて暗号化コンテンツデータ2090を復号し、その部分範囲を出力する範囲復号部2040、範囲復号部2040により出力された範囲復号コンテンツデータ2060、およびその部分範囲の復号されたコンテンツデータ2060を利用するコンテンツ利用機能2070が格納される。

【0038】コンテンツ利用部分選択部2030は、例えば、対象とするデータが電子書籍のデータである場合には利用者に読みたいページ番号を選択させ、また対象データが映像データである場合は利用者に視聴したい時間区間を選択させるような、コンテンツデータの中から利用したい部分を選択させる手段を提供する。このコンテンツデータの部分範囲の選択方法として、検索サーバ2400を用いて、利用者が入力した検索キーワードによりDB検索を行い、検索キーワードに該当するコンテンツデータの範囲を取得する方法がある。すなわち、データ販売システムとして、利用者がDB検索を行い、その結果に該当するコンテンツデータを購入するシステム形態である。

【0039】また、別の実施形態のシステムとして、利用者に配布した暗号化コンテンツデータ2090を利用者が試写・試聴して、利用する範囲を選択するシステムも考えられる。例えば、扱うコンテンツデータが映像データの場合において、利用者が映像データを編集して番組制作などに利用する目的で使用する場合を考える。このとき、あらかじめ配布する暗号化コンテンツデータ2090に対し、各フレーム画像に可視透かしを挿入して配布する。こうすることにより、配布映像データは試写・仮編集用途では用いることができるが、番組制作などの本編集用途では使用できないようになっている。利用者は、可視透かしの入った映像をコンテンツ利用部分選択手段2030で試写しながら映像の利用部分を決定し、その部分の可視透かしを取り去る範囲復号キーの取得要求を出す。そして復号キー取得し、その復号キーを用い利用部分の可視透かしを取り除いて本編集用途で使用する。

【0040】コンテンツ利用機能2070は、電子書籍データのページを表示するビューア、または映像データを再生するプレイヤなどと同等のものであり、コンテンツデータを利用者に利用させる機能を有する。

【0041】データセンタ2200は、コンテンツデータの管理や利用者の管理などを行うためのプログラムを格納する二次記憶装置2210、メモリ2320、CPU2330、およびネットワークインターフェース2340を備え、これら各部はバス2350で接続されてい

る。

【0042】二次記憶装置2210には、OS2260、販売するためのコンテンツデータ2240、それを利用者へ配布する際に暗号化する暗号化部2220、その暗号キー2250、暗号化したコンテンツを利用者へ配布するコンテンツ配布部2230、利用者に配布したコンテンツデータとそれに対応する復号キーを管理する復号キー管理テーブル2290、利用者から要求されたコンテンツデータの部分範囲を復号するキーを作成する範囲復号キー生成部2270、それにより生成された範囲復号キー2280、復号キー生成に連携して課金を行う課金部2300、および利用者に対する課金の状況を管理する課金管理テーブル2310が格納される。

【0043】検索サーバ2400は、コンテンツデータの範囲情報などを格納する二次記憶装置2410、メモリ2450、CPU2460、およびネットワークインターフェース2470を備え、これら各部はバス2480で接続されている。

【0044】二次記憶装置2410には、OS2440、コンテンツデータの範囲を管理するコンテンツ情報テーブル2430、コンテンツ情報テーブル2430を用いてコンテンツの範囲検索を行うコンテンツ範囲検索部2420が格納される。

【0045】以降では、図2に示すコンテンツデータ販売システムにおいて、扱うコンテンツデータが映像データの場合について、本発明の実施形態を説明する。

【0046】図3は、図2で示されるコンテンツデータ販売システムにおける各機能モジュールの関連とデータの流れを示している。図3を用いて、コンテンツデータの部分範囲の販売方法について説明する。

【0047】コンテンツデータ販売システムの全体処理の流れは次の通りである。本実施形態におけるコンテンツデータの販売システムでは、利用者はコンテンツデータを提供・管理するデータセンタ2200と契約する。そして、データセンタ2200は、契約した利用者に対し、あらかじめ暗号化されたコンテンツデータを配布する。利用者は、検索サーバ2400を用いて利用したいコンテンツデータをキーワード検索する。利用者は、検索結果に対応する暗号化コンテンツデータを復号する復号キーをデータセンタから購入する。そして、配布されている暗号化コンテンツデータの中の利用したいコンテンツデータに対し、復号キーを用いてデータを復号化し利用する。

【0048】コンテンツデータの配布に際しては、まずデータセンタ2200において、暗号化部2220により、暗号キー2250を使い配布対象のコンテンツデータ2240を暗号化する。暗号化部2220は、暗号化したコンテンツデータの識別子であるコンテンツIDとそのコンテンツを復号するための復号キーを復号キー管理DB2620へ格納する。この情報は、配布した暗号

化コンテンツを復号する範囲復号キー作成時に用いられる。暗号化したコンテンツは、コンテンツ配布部2230によって利用者端末2000に配布される。配布された暗号化コンテンツ2090は、利用者端末2000に接続されている二次記憶装置2080に格納される。コンテンツ配布部2230による配布の方法は、上述した通り、データを大容量メディアに格納して陸送する方法や、コンテンツ販売端末により利用者にダウンロードさせる方法などがある。

【0049】利用者は、コンテンツ利用部分選択部2030を用い、希望するコンテンツデータの検索を行う。コンテンツ利用部分選択部2030は、検索サーバ2400のコンテンツ範囲検索部2420へ、利用者より入力されたコンテンツデータ検索キーワードを渡し、コンテンツデータの検索を依頼する。コンテンツ範囲検索部2420は、コンテンツ情報DB2610のデータを用い、検索キーワードに合うコンテンツデータのコンテンツIDとその範囲情報を取得する。これにより、利用者は利用を希望するコンテンツデータの情報を取得する。

【0050】次に、利用者は、利用したいコンテンツデータに対し、そのデータを復号する復号キーを購入する。範囲復号キー取得部2050は、コンテンツ利用部分選択部2030により選択されたコンテンツデータのコンテンツIDとその範囲情報を用い、データセンタ2200にそのコンテンツの部分範囲を復号する範囲復号キーの作成を依頼する。データセンタ2200の範囲復号キー生成部2270は、そのコンテンツIDに対する全体復号キーを復号キー管理DB2620から取得し、これと範囲情報を組み合わせて範囲復号キー2280を作成する。この際、課金部2300を用いて範囲復号キーに対する課金処理を行う。これにより、利用者に対して範囲復号キーを渡し暗号化コンテンツの部分範囲を利用させることができ、さらにデータセンタ側でコンテンツデータの部分範囲の利用料を徴収することができる。

【0051】利用者は、範囲復号キー取得部2050により取得した範囲復号キーにより範囲復号部2040を用い、部分範囲のみ復号化した範囲復号コンテンツデータ2060を取得する。コンテンツ利用機能2070を使って、取得した範囲復号コンテンツデータを利用する。

【0052】以上の処理により、利用者にあらかじめ配布された暗号化データに対して、利用者が必要とする部分のみを利用させることができ、またその利用部分に応じた利用料を課金することができる。

【0053】図4は、映像データの場合におけるデータの暗号化と部分範囲の復号化の方式を示す概念図である。図4を用いて、映像データにおけるデータ暗号化・復号化方式を説明する。元映像データ3000は、販売対象となるデータであり、図3のコンテンツデータ2240に相当する。映像データ3000は、フレーム画像

3010～3070の集合データと見なすことができる。図3の暗号化部2220は、各フレーム画像3010～3070に対し同一キーで暗号化を施し、暗号化フレーム画像3110～3170を作成する。これら暗号化フレーム画像3110～3170を組み合わせ、暗号化映像データ3200を作成する。この暗号化映像データ3200を利用者へ配布する。これは、図3の暗号化コンテンツデータ2090に相当する。

【0054】コンテンツ利用部分選択部2030により、時間の形式で示される映像データの範囲3210が選択され、この範囲を復号する範囲復号キーが生成されることになる。範囲復号部2040は、範囲復号キーを用いその中に含まれる範囲情報3210に従い、その範囲に含まれるフレーム画像3220～3240を抜き出す。そして、フレーム画像3220～3240を復号化して、復号化フレーム画像3250～3270を作成する。このフレーム画像3250～3270を組み合わせ、範囲復号映像データ3300を作成する。

【0055】図5に、復号キー管理テーブル2290の例を示す。ここでは、コンテンツデータが映像データの場合を例として示す。復号キー管理テーブル3500は、映像データを識別する値であるコンテンツID3510と、そのデータを復号する復号キー3520と、そのデータの全範囲の大きさを示す先頭時間3530と、終了時間3540とから構成される。例えば、レコード3550は、「H100081101.mpg」という映像ファイルに対し、その復号化キーは「982E8BD」であることを示し、またそのデータは、先頭が「00:00:00:00」から始まり「01:20:00:00」で終了する1時間20分の長さの映像データであることを示している。ここで、映像の時間を示す値「a a : b b : c c : d d」は、a a時間b b分c c秒のd dフレーム目を示し、映像の位置をフレーム単位で特定することができる表記法である。

【0056】コンテンツデータの暗号方式は、復号キーを用いて復号可能な方式であれば、本発明に適用可能である。本実施形態では、7桁の16進数値で復号できる暗号を用いている。

【0057】復号キー管理テーブル2290には、データセンタ2200において利用者へコンテンツデータを配布するためにデータの暗号化を行った際に、暗号化したデータのデータ名とそのデータの復号キーとデータの範囲とを追加する。復号キーは、利用者に配布するコンテンツデータごとに変更し、配布したデータとその暗号を復号するキーの対応を復号キー管理テーブル2290で管理している。コンテンツデータごとにキーを変更することにより、あるコンテンツデータに対する復号キーが漏洩しても、他のコンテンツデータの安全性は保つことができる。

【0058】図5に示すように、復号キー管理テーブル

3500に、コンテンツデータ範囲の大きさ情報3530、3540を含むことにより、利用者からのコンテンツデータの部分範囲復号要求時に、その要求範囲が元のコンテンツデータの範囲に含まれているかの妥当性をチェックすることができる。

【0059】図6に、範囲復号キー2280のデータ構造を示す。範囲復号キー2280は、コンテンツデータを識別するコンテンツID3620、そのコンテンツデータを復号する復号キー3630、およびコンテンツデータの部分範囲を示す値とで構成される。本実施形態では、映像データを扱うため、コンテンツデータの部分範囲を示す値は、開始時間3640、終了時間3650で構成される。

【0060】図6の例では、「H100081101.mpg」という映像ファイルに対し、それを復号化するキーは「982E8BD」であり、そしてその映像ファイルを復号化する範囲は開始時間「00:20:30:15」から終了時間「00:22:10:07」までの区間であることを示している。

【0061】図7に、コンテンツ情報テーブル2430の例を示す。コンテンツ情報テーブル2430は、利用者が利用したいコンテンツを検索するためのコンテンツ内容のキーワードを格納した映像内容情報3700、コンテンツ内容キーワードに対応するコンテンツを識別するコンテンツID3710、およびキーワードに対応するコンテンツデータの範囲情報から構成される。本実施形態では、映像データを扱うため、コンテンツデータの範囲情報は、開始時間3720と終了時間3730で構成される。例えば、レコード3740では、映像内容のキーワードとして「春」、「青空」、「桜の花」、「名古屋城」に対応する映像データは、ファイル名「H10081101.mpg」の開始時間「00:20:30:15」から終了時間「00:22:10:07」の部分であることを示している。

【0062】図8に、課金管理テーブル2310の例を示す。課金管理テーブル2310は、課金に対する契約を識別する契約ID3800、課金対象の利用者を識別する利用者ID3810、および課金の料金3820で構成される。課金は、範囲復号キーを発行する度に行う。範囲復号キー発行により、利用者に対し利用したい範囲のみを復号化し提供しているので、その範囲のみの利用料を課金することができる。

【0063】次に図9から図11のフローチャートに基づいて、本実施形態のシステムにおけるコンテンツデータ復号化の処理の流れを説明する。

【0064】図9は、範囲復号キー取得部2050の処理手順を示すフローチャートである。

【0065】まず、コンテンツ利用部分選択部2030から復号するコンテンツデータのコンテンツデータIDと範囲を受け取る（ステップ4010）。本ステップよ

り前に、コンテンツ利用部分選択部2030とそれに関する機能ブロックにより次のような処理が行われるものとする。コンテンツ利用部分選択部2030は、利用者がコンテンツデータの利用したいデータ名とその範囲とを決定する手段を提供するもので、前述のように種々の方法を用いてよい。本実施形態では、検索サーバ2400のコンテンツ検索部2420を用いてデータ名と範囲を取得する。例えば、利用者が「名古屋城」の映像が欲しいと思った場合、利用者は、コンテンツ利用部分選択部2030に検索キーワード「名古屋城」を渡す。コンテンツ利用部分選択部2030は、コンテンツ範囲検索部2420にキーワード「名古屋城」を渡しコンテンツデータの検索を依頼する。コンテンツ範囲検索部2420は、コンテンツ情報テーブル2430を用い、キーワード「名古屋城」が映像内容情報3700に一致するレコード3740を取得し、そのコンテンツID「H100081101.mpg」と開始時間「0:20:30:15」と終了時間「0:22:10:07」をコンテンツ利用部分選択部2030に返す。コンテンツ利用部分選択部2030は、そのデータ名と範囲情報を範囲復号キー取得部2050に渡す。

【0066】次に、受け取ったコンテンツデータIDと範囲を、範囲復号キー生成部2270に渡して範囲復号キーの生成を依頼し、その結果として範囲復号キーを得する(ステップ4020)。

【0067】さらに、範囲復号キーを範囲復号部2040に渡し、コンテンツデータ範囲復号要求を出す(ステップ4030)。この範囲復号キーの生成処理とコンテンツデータの範囲復号処理を、以下に説明する。

【0068】図10を用いて、範囲復号キーの生成手順を説明する。図10は、範囲復号キー生成部2270の処理手順を示すフローチャートである。

【0069】まず、範囲復号キー取得部2050からコンテンツIDと範囲を受け取る(ステップ4110)。このコンテンツIDを用いて、復号キー管理テーブル3500からそのコンテンツIDに対応するデータの復号キーとそのデータの全体の範囲を取得する(ステップ4120)。例えば具体的には、復号キー管理テーブル3500のコンテンツID「H100081101.mpg」に対応するレコード3550を取得し、その復号キー「3520「982E8BD」、データ全体範囲として先頭時間3530「00:00:00:00」、終了時間3540「01:22:00:00」を取得する。

【0070】次に、範囲復号キー取得部2050から受け取った範囲が、復号キー管理テーブル3500から取得した全体範囲3530、3540の中に入っているかを調べる(ステップ4130)。例えば具体的には、部分範囲として開始時間「00:20:30:15」から終了時間「00:22:10:07」の範囲は、映像データ「H100081101.mpg」の全体範囲「0:

0:00:00:00」～「01:20:00:00」の中に含まれているので、要求された範囲は正しいと認める。

【0071】コンテンツID、復号キー、および範囲を組み合わせ、範囲復号キー本体を作成する(ステップ4140)。例えば具体的には、コンテンツID「H100081101.mpg」、開始時間「00:20:30:15」、終了時間「00:22:10:07」に対して、全体復号キー「982E8BD」を付加して、図6の範囲復号キー本体3600のデータを作成する。

【0072】範囲復号キー2280の発行に連携して課金処理を行う(ステップ4150)。課金処理は、課金部2300に依頼して行う。課金処理において課金対象となる利用者が判別できるように、利用者がデータを利用する前にログインするシステム構成にしておく。または、範囲復号キー取得部2050が範囲復号キー生成を依頼する際に利用者IDも送付するなどの仕組みにしておく。

【0073】作成した範囲復号キー2280を範囲復号キー取得部2050へ渡し(ステップ4160)、処理を終了する。

【0074】図11を用いて、コンテンツデータの範囲復号処理を説明する。図11は、範囲復号部2040の処理手順を示すフローチャートである。

【0075】まず、コンテンツIDに対応する暗号化コンテンツデータ2090を取得する(ステップ4220)。コンテンツデータは二次記憶装置2080に格納されており、ここではDVD-ROMなどの大容量メディア、または販売端末でダウンロードするための読み書き可能なリムーバブルメディアを想定している。従つて、必要に応じてメディアの交換を行う。すなわち、コンテンツIDに対応するコンテンツデータ2090を格納するメディアをドライブに挿入し読み出し準備を行ったのち、必要な暗号化コンテンツデータ2090を取得する。

【0076】続いて、暗号化コンテンツデータ2090から部分データを取り出す。具体的には、図4に示すような暗号化映像データ3200から、部分データとして個々のフレーム画像3110～3170を一つずつ取り出す(ステップ4230)。一つずつ順番に取り出したフレーム画像に対し、範囲復号キー2280の範囲情報3640、3650の範囲に含まれるかをチェックする。具体的には、図6に示す範囲復号キーの例の場合には、取り出したフレーム画像が「00:20:30:15」から「00:22:10:07」に含まれているかを調べる(ステップ4240)。範囲3640、3650に含まれるフレーム画像は、範囲復号キー2280の中の全体復号キー3630を用いて復号化する(ステップ4250)。範囲3640、3650に含まれないフレーム画像は破棄する(ステップ4260)。かかる処

理（ステップ4230～4250）を映像データを構成する全てのフレーム画像について繰り返す（ステップ4270）。

【0077】ステップ4250で復号化された部分データを組み直し、範囲復号化コンテンツデータ2060を作成し出力する。具体的には、図4に示すように復号化されたフレーム画像3250, 3260, 3270を用い、このフレーム画像で構成される映像データ3300を作成し（ステップ4280）、処理を終了する。

【0078】以上の処理により、暗号化コンテンツデータ2090と範囲復号キー2280から部分範囲のみを復号化したデータを出力することができる。

【0079】次に、図12および図13を参照して、本発明のデータ暗号化・復号化方式の第2の実施の形態を説明する。なお、第2の実施の形態において、第1の実施の形態と同様の部分は説明を省略する。

【0080】図12は、第2の実施の形態の範囲復号方式の概念図である。この範囲復号方式は、第1の実施の形態の暗号化データ1200とは異なる形式のデータに対する範囲復号方式である。暗号化データ1000は、データ全体が暗号化されているデータである。また、暗号化データ1000は、その暗号化前のデータが任意の部分範囲を切り出すことができるデータである。第1の実施形態の暗号化データ1200は部分単位暗号データ1280の集合として表されるのに対し、第2の実施形態の暗号化データ1000は暗号化データの集合ではなく1つの暗号化データとして表現される。例えば、映像データを例に説明すると、第1の実施の形態では、映像データはフレーム画像の集合であり、各フレーム画像を暗号化した映像データとして扱っていた。第2の実施の形態では、映像データそのものを暗号化してしまい全体を1つの暗号データとして扱う方式を想定している。具体的には、映像データがMPEGファイルで表現されているときには、暗号化データ1000はMPEGファイル自体を暗号化したデータになる。

【0081】範囲復号装置1040は、図1と同様に暗号化データと範囲復号キー1010を受け取り、暗号化データの部分範囲1090を出力する。このとき用いる範囲復号キー1010は、第1の実施の形態と同様に、全体復号キー1020と復号範囲1030からなる。全体復号キー1020は、第1の実施の形態では暗号化データの個々の部分単位1280を復号化するキーであったのに対し、ここでは暗号化データ1000を復号化するキーである。復号範囲1030は、第1の実施の形態と同様の値をとる。例えば、電子書籍のデータの場合はページ番号であり、映像データの場合は時間である。復号範囲1030は、暗号化データ1000の部分範囲1000を示している。

【0082】範囲復号装置1040は、全体復号化部1050と範囲選択部1080を備える。全体復号化部1

050は、範囲復号キー1010の中の全体復号キー1020を用いて暗号化データ1000の復号化処理を行い、復号化データ1060を出力する。範囲復号キー1010の中の復号範囲情報1030は、復号化データ1060の中の部分範囲1070を示している。範囲選択部1080は、復号化データ1060から復号範囲情報1030で示される部分範囲を切り出し、復号化範囲データ1090を出力する。

【0083】図12では、復号化範囲データ1090として復号化したデータの部分範囲を切り出して出力しているが、これは暗号化データ全体の中で選択された部分範囲のみを復号化したデータでも良い。これは、暗号化データと出力される復号化データのデータの大きさは同じであり、復号キーで選択された部分のみ復号化されており、他の部分は暗号がかかったままのデータである。

【0084】図13を用いて、データ全体が暗号化されているデータに対する部分範囲復号化の処理を説明する。以下では、第2の実施の形態のデータ復号化方法を図2で示されるデータ販売システムに適用した場合を想定して、データ復号化方法の実施の形態を説明する。つまりは、図2の利用者端末2000にあらかじめ配布した暗号化コンテンツデータ2090がデータ全体が暗号化された暗号化データ1000であり、範囲復号部2040は暗号化データ1000を復号化するものである。図13は、この場合の範囲復号部2040の処理手順を示すフローチャートである。

【0085】まず、範囲復号キーに含まれるコンテンツIDに対する暗号化コンテンツデータ2090を取得する（ステップ4320）。これは、第1の実施の形態で説明した図11に示すフローチャートのステップ4220と同一の処理である。次に、暗号化コンテンツデータ2090を範囲復号キー1010の中の全体復号キー1020を用いてコンテンツデータ全体を復号化する（ステップ4330）。

【0086】復号化コンテンツデータから部分データを一つずつ取り出し（ステップ4340）、その部分データが範囲復号キー2280の中の範囲3640, 3650に含まれているかを調べる（ステップ4350）。具体的には、第1の実施の形態における図11と同様に、映像データのフレーム画像を取り出し、そのフレーム画像が該範囲に含まれているかを調べる。ここでは、第1の実施の形態における図11の方式とは違い、フレーム画像は既に復号化されている。選択範囲に含まれる部分データは出力し（ステップ4360）、選択範囲に含まれない部分データは破棄する（ステップ4370）。コンテンツデータに含まれる全ての部分データに対し前記の範囲チェックを行う（ステップ4380）。

【0087】以上の処理により、全体を暗号化したコンテンツデータに対しても、範囲復号キー2280を用いて部分範囲のみを復号化したデータを出力することがで

きる。

【0088】次に、図14～図17を参照して、本発明のデータ暗号化・復号化方式の第3の実施の形態を説明する。なお、第3の実施の形態において、第1の実施の形態と同様の部分は説明を省略する。

【0089】図14は、第3の実施の形態の範囲復号方式の概念図である。第3の実施形態の暗号化データの範囲復号方式は、サイン（署名）データ5010を付加した範囲復号キー5000を用いるものである。サインデータ5010は、全体復号キー1270と復号範囲1030の内容が正しいことを証明するためのデータであり、このサインデータ5010を検定することで範囲復号キーの改竄をチェックすることができる。これにより、あらかじめ配布された暗号化データ1200を範囲復号キーを捏造することによって不正に利用されることを防ぐことができる。サインデータの検定については下記に述べる。ここで、暗号化データ1200は第1の実施の形態と同様に部分単位暗号化データ1280の集合として表されるデータである。

【0090】範囲復号化装置5030は、サイン検定部5020と、範囲取得部1230と、復号化部1240を備える。範囲復号化装置5030は、第1の実施の形態と同様に、暗号化データ1200と範囲復号キー5000を入力とし、復号化範囲データ1250を出力する。暗号化データ1200と範囲復号キー5000が入力されると、まず範囲復号キー5000の中のサインデータ5010を、サイン検定部5020により検定し、範囲復号キー5000の正当性をチェックする。ここで範囲復号キー5000が正しくないと認められたら、範囲復号処理を中断し、復号化範囲データ1250を出力しない。これにより、不正な範囲復号キーの使用を防ぐことができる。サイン検定が行われた後、範囲取得部1230は、暗号化データ1200の中から選択範囲データ1210を抜き出し、復号化部1240は、選択範囲データ1210を復号化して復号化範囲データ1250を出力する。この処理は、第1の実施の形態で示した範囲取得部1230および復号化部1240の処理と同様である。

【0091】以下では、第3の実施の形態のデータ復号化方法を図2で示されるデータ販売システムに適用した場合を想定して、サイン付き範囲復号キー5000を用いるデータ復号化方法の実施の形態を説明する。つまりは、図2のデータセンタ2200の範囲復号キー生成部2270と利用者端末2000の範囲復号部2040が、サイン付き範囲復号キー5000を扱うよう処理が変更されているシステムである。

【0092】図15は、範囲復号キー5000のデータ構造を示す。範囲復号キー5000は、範囲復号キーの本体を格納する本体部分3600と、そのデータに対する発行元のデータセンタ2200のサイン（署名）を格

納するサイン部分3610で構成される。

【0093】データセンタのサイン3660を付加することにより、この範囲復号キー5000を受け取る範囲復号部2040は、範囲復号キー本体3600の改竄をチェックすることができる。すなわち、データセンタのサイン3660は、範囲復号キー本体3600をデータセンタ2200の秘密キーで暗号化したデータである。範囲復号部2040は、サイン3660をデータセンタ2200の公開キーで復号化し、その復号化したデータと範囲復号キー本体3600とが一致することを調べ、一致した場合には範囲復号キー本体3600は正しいデータであると認める。

【0094】範囲復号キー本体3600は、図6と同様に、コンテンツデータを識別するコンテンツID3620、そのコンテンツデータを復号する復号キー13630、およびコンテンツデータの範囲を示す値で構成される。本実施の形態では映像データを想定しているため、コンテンツデータの範囲を示す値は開始時間3640と終了時間3650で構成される。

【0095】図16を用いて、サイン付き範囲復号キー5000の作成処理を説明する。サイン付き範囲復号キー5000の作成手順は、第1の実施の形態における図10の範囲復号キー2280の作成手順とほぼ同じである。まず、範囲復号キー取得部2050からコンテンツIDと範囲を受け取る（ステップ4410）。このコンテンツIDを用いて復号キー管理テーブル3500から当該コンテンツIDに対応するデータの全体復号キーとそのデータの全体の範囲を取得する（ステップ4420）。範囲復号キー取得部2050から受け取った範囲が、復号キー管理テーブル3500から取得した全体範囲3530、3540の中に含まれているかを調べる

（ステップ4430）。コンテンツID、復号キー、および範囲を組み合わせ、範囲復号キー本体3600を作成する（ステップ4440）。ここまででは、第1の実施の形態の図10に示すステップ4110～ステップ4140と同様である。

【0096】次に、前ステップまでに作成された範囲復号キー本体3600に対し、データセンタ2200の秘密キーでサインする（ステップ4450）。具体的には、範囲復号キー本体3600に対し、図15に示すように、サインデータ3660が付加されることになる。つづいて、サイン付き範囲復号キー5000の発行に連携して課金処理を行い（ステップ4460）、作成したサイン付き範囲復号キー2280を範囲復号キー取得部2050へ渡す（ステップ4470）。このステップは、第1の実施の形態における図10のステップ4150およびステップ4160と同様である。

【0097】図17を用いて、サイン付き範囲復号キー5000を用いて暗号化データの部分範囲を復号する処理を説明する。

【0098】まず、範囲復号キー取得部2050から範囲復号キーを受け取り、サインの検定を行う。サインの検定により、範囲復号キーが正しくないと認められた場合はデータの復号化を中止する(ステップ4510)。サインの検定に用いるデータセンタ2200の公開キーは、範囲復号部2040にあらかじめ埋め込んでおくか、または外部の認証局から取得するなどの方法で取得する。

【0099】サインの検定後のデータの部分範囲の復号化処理は、第1の実施の形態における図11のデータの部分範囲の復号化処理と同様の処理である。

【0100】まず、コンテンツIDに対応する暗号化コンテンツデータ2090を取得する(ステップ4520)。続いて、暗号化コンテンツデータ2090から部分データを取り出す(ステップ4530)。一つずつ順番に取り出したフレーム画像に対し、範囲復号キー2280の範囲情報3640、3650の範囲に含まれるかをチェックする(ステップ4540)。範囲3640、3650に含まれるフレーム画像は範囲復号キー2280の中の全体復号キー3630を用いて復号化する(ステップ4550)。範囲3640、3650に含まれないフレーム画像は破棄する(ステップ4560)。かかる処理を映像データを構成する全てのフレーム画像について繰り返す(ステップ4570)。ステップ4550で復号化された部分データを組み直し、範囲復号化コンテンツデータ2060を作成し出力する(ステップ4580)。ここまで処理は、第1の実施の形態における図11のステップ4220～ステップ4280と同様の処理である。

【0101】以上の処理により、サイン付き範囲復号キー5000を用いて、範囲復号キーの改竄を防ぐことができる。

【0102】第3の実施の形態では暗号化データとして部分単位暗号化データ1280の集合として表されるデータを用いた例を説明したが、第2の実施の形態の方式を第2の実施の形態で示した全体を暗号化した暗号化データ1000に適用することもできる。すなわち、第2の実施形態に対してサインによる検定処理を適用できる。

【0103】また第3の実施の形態では、データの改竄を防止する方法として、範囲復号キー本体3600にサインデータ3660を付加し、それを検定することでデータの改竄を防止していたが、範囲復号キー本体3600をデータセンタ2200と範囲復号部2040と共に共有する秘密キーで暗号化する方法を用いても良い。すなわち、共有する秘密キーを用いてデータセンタ2200で範囲復号キーを暗号化し、同じく共有する秘密キーを用いて範囲復号部2040で復号化する。これにより、暗号化した範囲復号キーを改竄すると範囲復号部2040で正しく範囲復号キーの復号ができず、暗号化データ

を復号することができなくなる。また、この方式では範囲復号部2040ごとに共有秘密キーを変更することにより、ある特定の範囲復号部2040に対してのみ暗号化データの復号化ができる範囲復号キーを作成することができる。

【0104】さらに、上述した範囲復号キー本体3600をデータセンタ2200と範囲復号部2040が共有する秘密キーで暗号化したデータに対し、データセンタ2200のサインを付加することにより、より堅牢なシステムを構成することができる。すなわち、範囲復号キー本体3600を暗号化する共有秘密キーが漏洩した場合にも、サインデータ3660による検定が行われるため範囲復号キーを捏造することができない。また、逆にデータセンタの秘密キーが漏洩した場合にも、共有秘密キーが分からなければ範囲復号キーを生成することができない。

#### 【0105】

【発明の効果】以上述べたように、本発明によれば、暗号化データの部分範囲のみを復号化(全体を復号化し部分範囲のみを利用者に渡す方式も含む)するような復号キーが作成でき、この復号キーを用いて暗号化データの部分範囲のみを復号化することができる。この復号キーと復号化装置により、あらかじめ利用者にデータを配布するようなデータ販売システムにおいても、データの部分範囲のみの販売ができる。従って、利用者にあらかじめ配布された暗号化データに対して、利用者が必要とする部分のみを利用させることができ、またその利用部分に応じた利用料を課金することができる。サイン付き範囲復号キーを用いるようにすれば、範囲復号キーの改竄を防ぐことができる。

#### 【図面の簡単な説明】

【図1】本発明の第1の実施の形態のデータ復号化方法の概念図である。

【図2】第1の実施形態のデータ復号化方法を用いたコンテンツ販売システムのシステムブロック図である。

【図3】第1の実施形態のデータ復号化方法を用いたコンテンツ販売システムの機能ブロックの関連とデータの流れを示す図である。

【図4】第1の実施形態を映像データに適用した場合におけるデータの暗号化・復号化処理の概念図である。

【図5】復号キー管理テーブルの例を示す図である。

【図6】範囲復号キーのデータ構造を示す図である。

【図7】コンテンツ情報検索テーブルの例を示す図である。

【図8】課金管理テーブルの例を示す図である。

【図9】範囲復号キー取得部における範囲復号キー取得処理のフローチャート図である。

【図10】範囲復号キー生成部における範囲復号キー生成処理のフローチャート図である。

【図11】範囲復号部におけるコンテンツデータに対する

る部分範囲の復号化処理のフローチャート図である。

【図12】本発明の第2の実施の形態のデータ復号方法の概念図である。

【図13】第2の実施の形態の範囲復号部における部分範囲の復号化処理のフローチャート図である。

【図14】本発明の第3の実施の形態のサイン付き範囲復号キーによるデータ復号化の概念図である。

【図15】サイン付き範囲復号キーのデータ構造を示す図である。

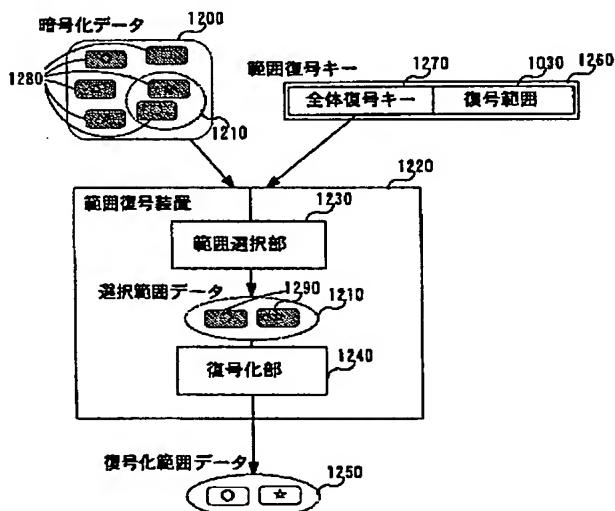
【図16】サイン付き範囲復号キー生成処理のフローチャート図である。

【図17】サイン付き範囲復号キーを用いたデータの部分範囲の復号化処理のフローチャート図である。

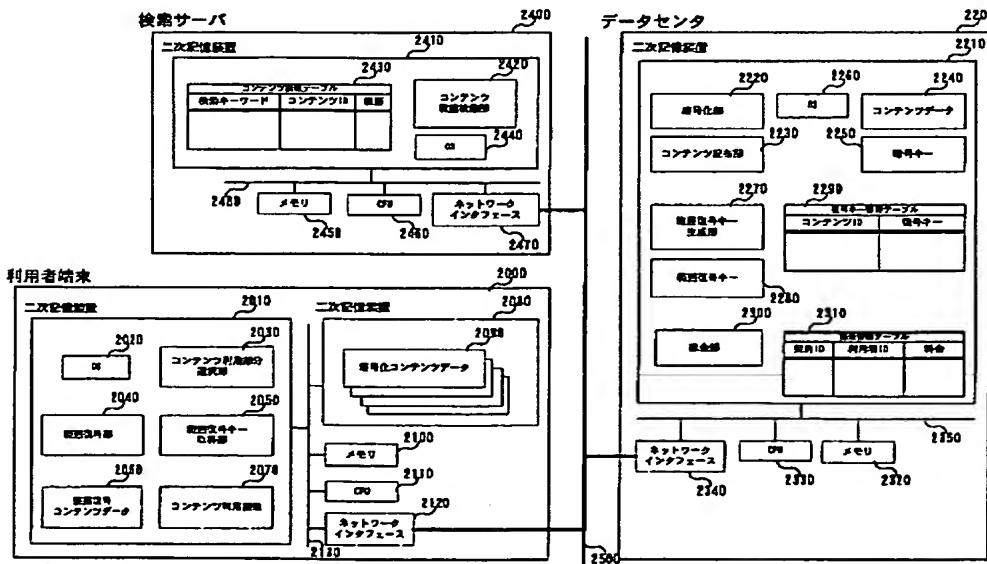
#### 【符号の説明】

- 1000……暗号化データ
- 1200……集合形式の暗号化データ
- 1260……範囲復号キー
- 1270……全体復号キー
- 1260……復号範囲情報
- 1250……復号化範囲データ
- 2030……コンテンツ利用部分選択部
- 2040……範囲復号部
- 2050……範囲復号キー取得部
- 2270……範囲復号キー生成部
- 2300……課金部
- 5000……サイン付き範囲復号キー

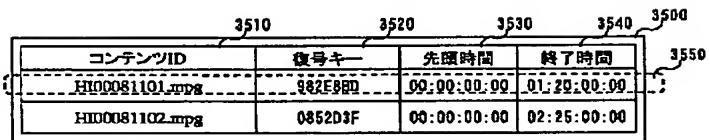
【図1】



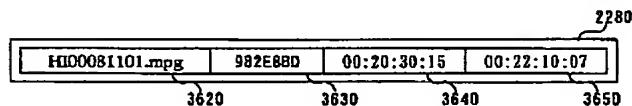
【図2】



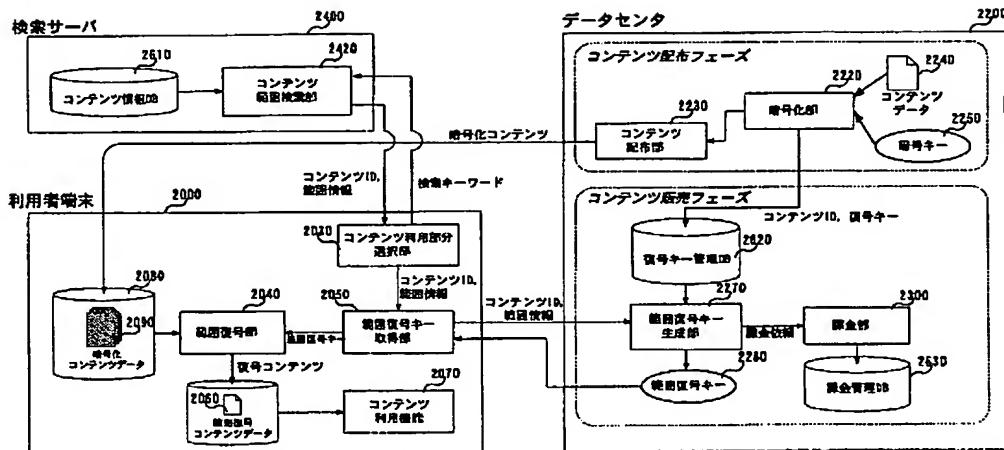
【図5】



【図6】



【図3】



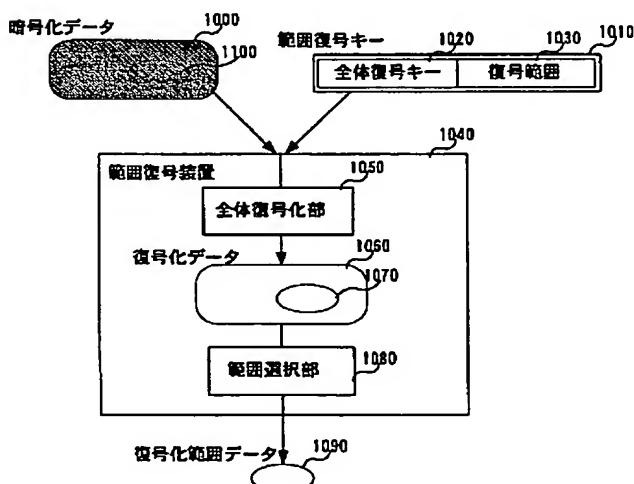
【図7】

映像内容情報	コンテンツID	開始時間	終了時間
春、青空、桜の花、名古屋城	HD00081101.mpg	00:20:30:15	00:22:10:07
夏、市街、ハイビスカス、太陽	HD00081102.mpg	00:01:00:00	00:03:29:17

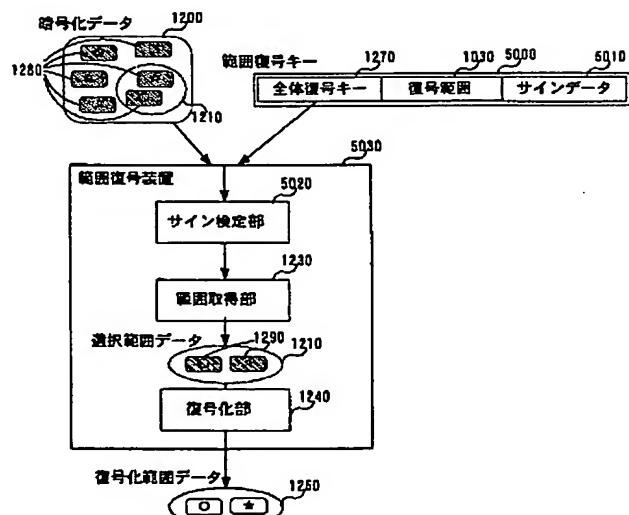
【図8】

契約ID	利用者ID	料金
208015	AB00001	¥10,000

【図12】



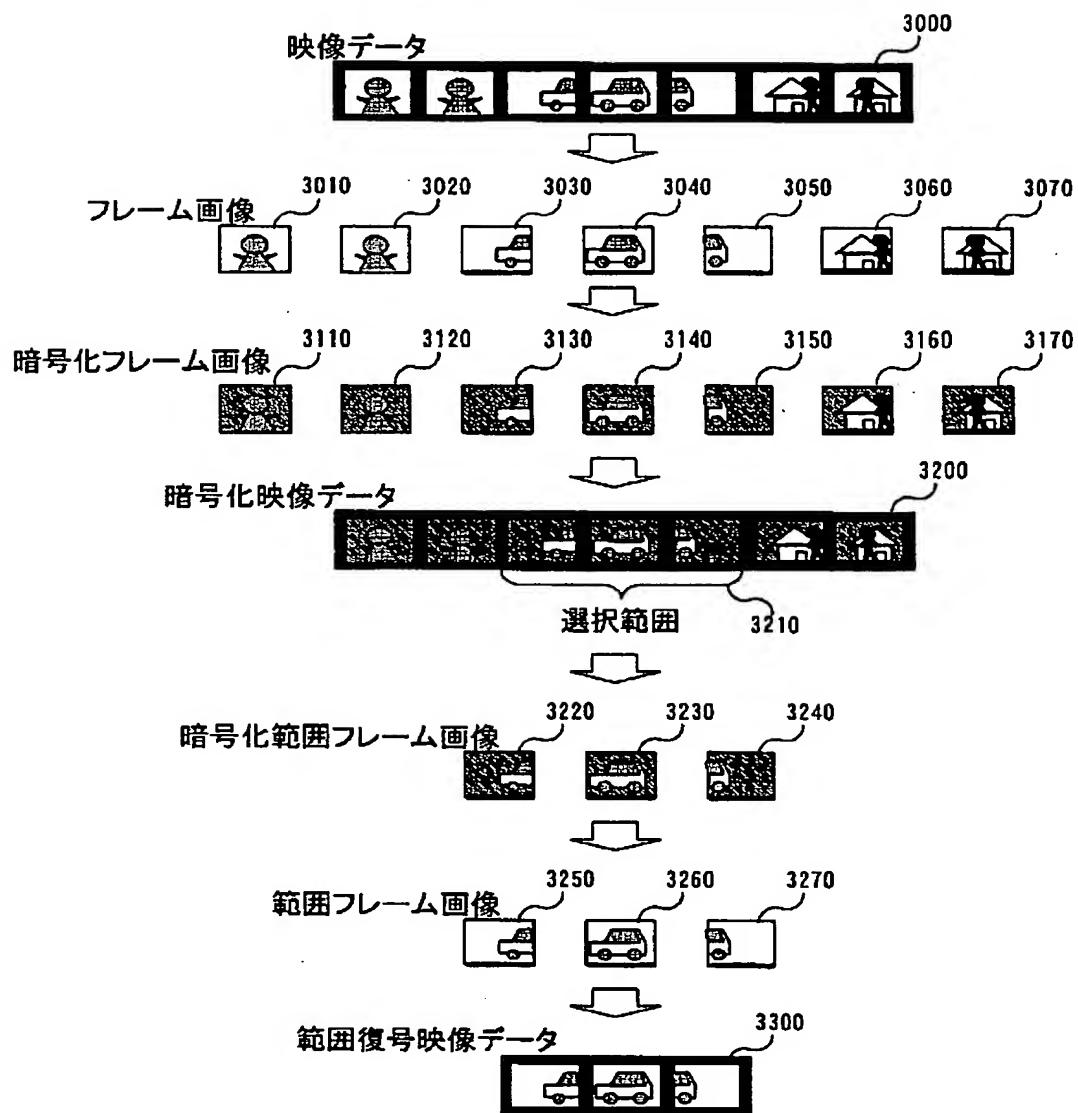
【図14】



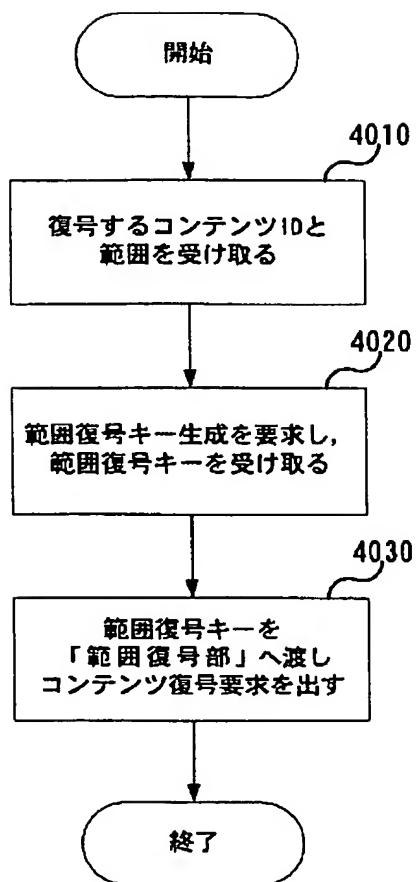
【図15】

HD00081101.mpg	982E8BD	00:20:30:15	00:22:10:07	6DB0HMD4ADE100ADC98085X8FGAKP0QK5D
3620	3630	3640	3650	3660

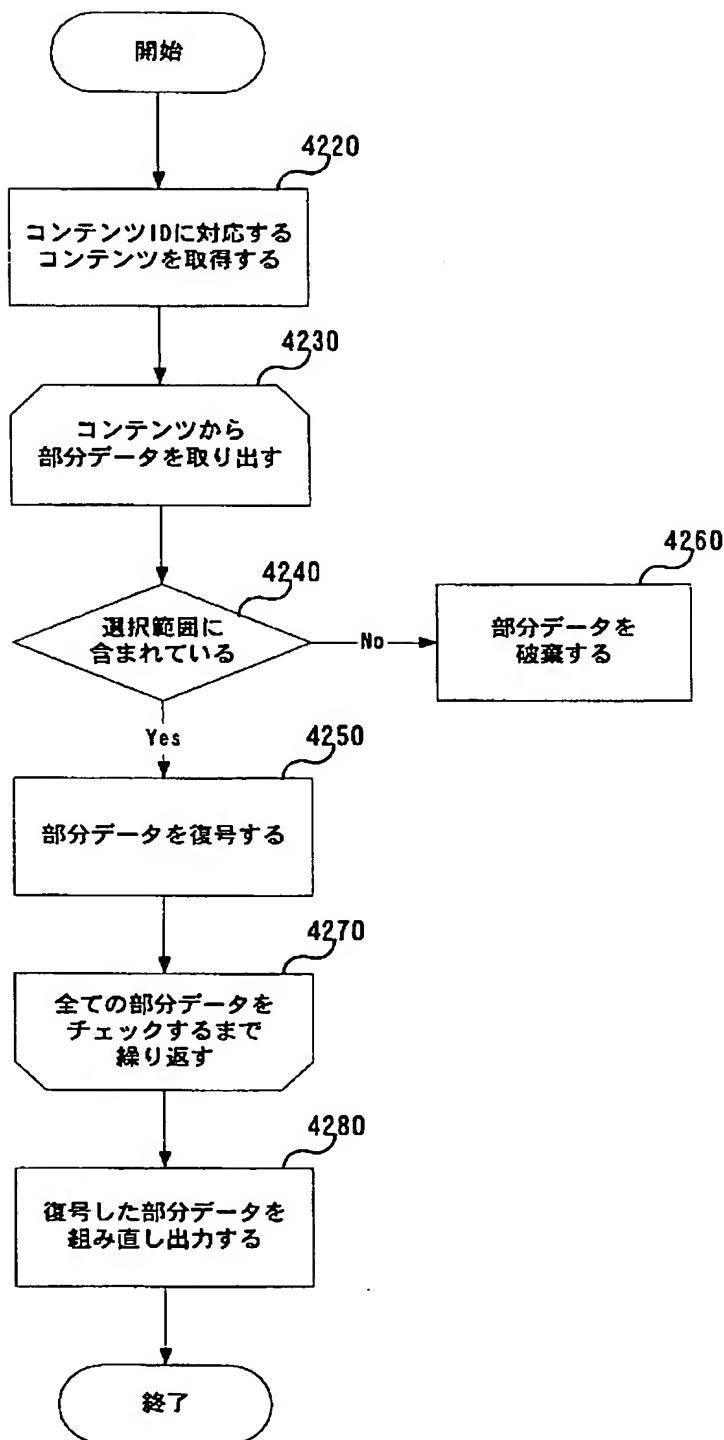
【図4】



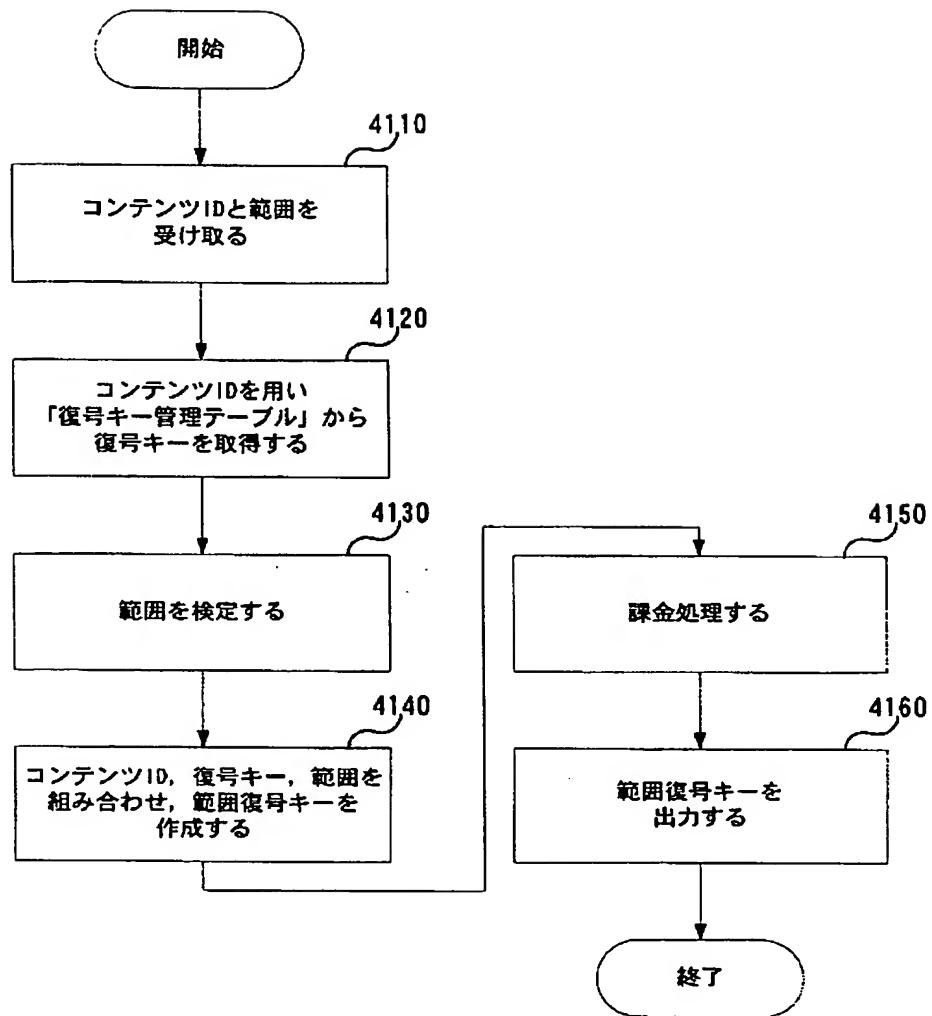
【図9】



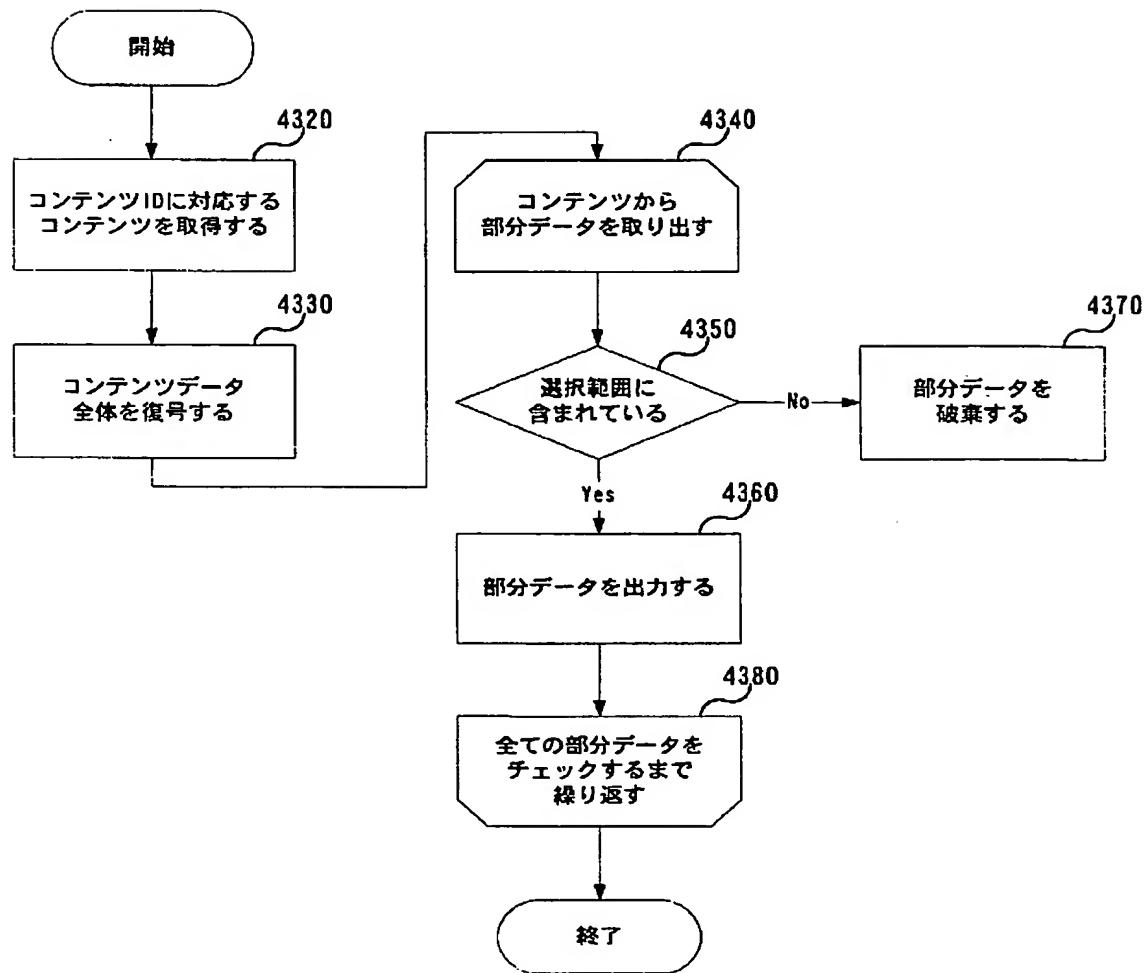
【図11】



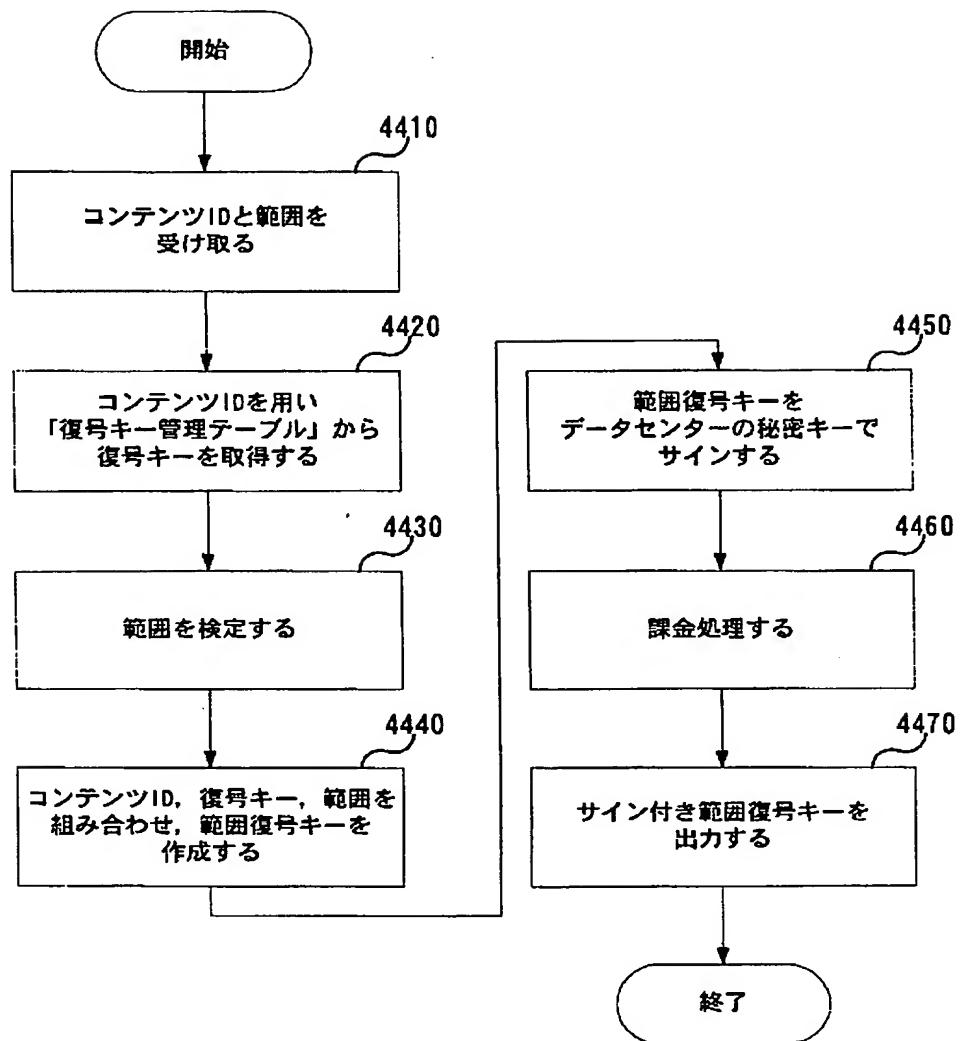
【図10】



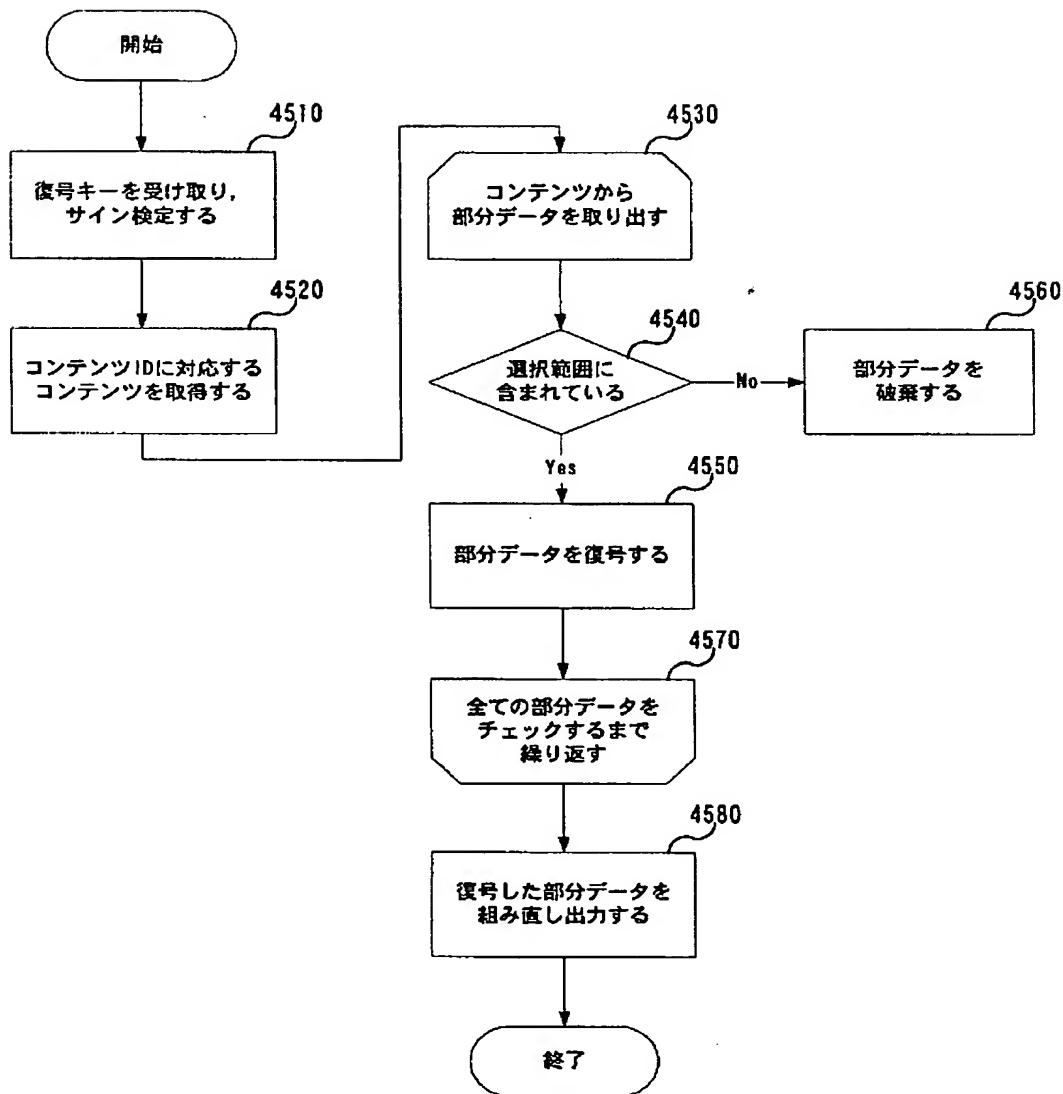
【図13】



【図16】



【図17】



フロントページの続き

(72)発明者 岩崎 一正

神奈川県川崎市幸区鹿島田890番地 株式  
会社日立製作所ビジネスソリューション事  
業部内

(72)発明者 小林 り恵

神奈川県川崎市幸区鹿島田890番地 株式  
会社日立製作所ビジネスソリューション事  
業部内

(72)発明者 小池 博

神奈川県川崎市幸区鹿島田890番地 株式  
会社日立製作所ビジネスソリューション事  
業部内

(72)発明者 鳩岡 順一

神奈川県横浜市戸塚区戸塚町5030番地 株  
式会社日立製作所ソフトウェア事業部内

F ターム(参考) 5J104 AA01 AA16 EA04 EA15 NA02